Volume 15, Issue 09   Atari Online News, Etc.   March 1, 2013

=~=~=~=

A-ONE #1509   03/01/13

~ Tech Lobbying Efforts! ~ People Are Talking!   ~ Atari to Activision!
~ Win 8 Fails To Impress! ~ Death, Facebook Photos ~ Chromebook Pixel!
~ Cybersecurity Talks!   ~ GameSpy, 1UP Are Gone! ~ The Activisionaries!

~ Text-based CAPTCHA Dead ~ IE 10 for Win 7 Here! ~ UK Grandparents Out?

-* China Accuses US of Hacking! *-
-* Spyware Images Sent to Rental PCs! *-
-* Apple's Deleting Emails Containing "Porn"? *-

=~=~=~=

->From the Editor's Keyboard   "Saying it like it is!"
  """"""""""""""""""""""""""""

Well, we apparently dodged a bullet last weekend, and did not have a
third weekend of a wintry storm. Yes, we got a little bit of snow, but
it was more an "inconvenience" snowfall than anything else. The little
bit that we had was cleaned up very quickly, and residual snow melted in
a day or so. Hopefully, we've seen the worst of this season's snow.

A lot of interesting articles are included in this week's issue, including
a number of "history-making" items related to the gaming industry' past
and present. I hope that you'll enjoy them.

Untikl next time...

=~=~=~=

->In This Week's Gaming Section - PlayStation 4 Games Warn of PS-Style Surveill
ance!
  """""""""""""""""""""""""""""   PS4, Next-gen Xbox Can t Compete with PCs!
                                   Activisionaries Changed the Industry!
                                   And much more!

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!
  """""""""""""""""""""""""""""""""""

          Playstation 4 Games Warn of PS-Style Surveillance

The debut of the PlayStation 4 in New York City Wednesday (Feb. 20) was as
remarkable for what it showed as for what it didn't show: Sony unveiled a
raft of beautiful, incredibly realistic new games, but not the console
itself. The device, perhaps in a straight-from-the-lab rough appearance,
was somewhere offstage, driving the giant projectors that broadcast

previews of upcoming games around the Hammerstein Ballroom.

Out-of-site-yet-everywhere seems to be the overall metaphor of the PlayStation 4 (PS4), as Sony described it. The PS4 (which Sony plans to sell by year's end) is not so much a machine as a network   with games delivered from the cloud, games that can follow you as you move from the PS4 to a mobile device, and the ability to post video clips of your adventures or even broadcast entire games online.

"We're making it so your friends can look over your shoulder virtually and interact with you as you play," said David Perry, co-founder of Gaikai, a company that Sony bought to build its cloud-gaming network.

But not only friends will be watching. Sony will. "The PlayStation network will get to know you by understanding your personal preferences and the preferences of your community and turn this knowledge into useful information that will enhance your gameplay," Perry said.

Every important technology has good and bad uses. Some of the upcoming games that Sony showcased for the PS4 explore, perhaps unwittingly, the darker side of omnipresent, omniscient networks similar to what Sony is building.

Suckerpunch's new game "inFAMOUS: Second Son" explores the surveillance state. "Right now, there are 4.2 million security cameras distributed all around Great Britain. That's one camera for every 14 citizens," said game director Nate Fox, in a dramatic introduction to the game. "It is hard to put your finger on what that sense of security is worth, but it is easy to say what it costs   our freedom."

Like Great Britain, the PS4 will also have a vast network of cameras   not one for every 14 citizens, but one for every console owner. At the presentation, Marc Cerny, head of the PlayStation hardware platform, showed a photo of a depth-sensing stereo camera for the PS4, designed to track the new Dualshock controller as it moves.

The danger in "Second Son" is that some individuals have developed super-human powers (a la "Heroes") that make them living weapons. They carry no traditional weapons and show no physical signs of danger rendering all the modern surveillance tech impotent.

But what if new security technology could go beyond the physical? What if it could read people's intentions and predict their next moves?

What if it were like the PS4?

Sony believes that PlayStation owners simply give off so much data as they interact intensively with the console, other devices and the network that it can know what its users intend to do.

"People haven't' changed, but now everybody's broadcasting. And once you've seen it, all of it, how do you look away?"

That's not a quote from a Sony or game-company executive. It's from the lead character in the upcoming Ubisoft game "Watch Dogs." It follows a vigilante character with access to all that information. As he walks through Chicago, message windows pop up, showing details about the people he passes. Marcus Rhodes, a 43-year-old Iraq War veteran, is unemployed. Sandy Higgins, a grade-school teacher, recently won a child-custody battle and has a 30 percent chance of being a crime victim.

In the clip, the vigilante uses the knowledge to find a woman in danger and to track her attacker in a chase through the city. But as the police then pursue him, the game shows how much data the protagonist himself is giving off.

It's rather unlikely that the PlayStation 4 was designed to be a mass surveillance device, a Trojan Horse of a game console designed to slip spooks into the living room. Far likelier, Sony just wants the games to be more involving and better targeted for the customers, so they will buy and play more games.

"If we know enough about you to predict the next game you'll purchase, then that game can be loaded and ready to go before you even click the button," Marc Cerny said.

But still, the PS4 will collect a lot of information. That itself, in the right imagination, could be fodder for a good dystopian video game.

Crytek CEO: PlayStation 4, Next-gen Xbox Can t Compete with PCs

There may come a day when diehard video game fans ditch their consoles completely in favor of PC gaming. Following the unveiling of Sony s PlayStation 4 console, and just ahead of Microsoft s (MSFT) next Xbox s debut, the CEO of leading game lab Crytek offered Eurogamer a grim dose of reality: neither of these next-generation consoles can compete with PCs in terms of the technology that powers them.

 We used Moore s Law. If you predict how hardware evolves at the current speed of evolution, and then take consumer pricing evolution, already two years ago you could see, whatever launches in 2013 or 2014 or 2015, will never beat a PC again, Crytek boss Cevat Yerli told the site in a recent interview. The executive believes PC video games will remain the place to be for the best possible visuals.

And because technology advances so quickly, affordable PCs with far more impressive capabilities than the PS4 and next-gen Xbox will be available to consumers long before any follow-ups Sony and Microsoft may be brewing see the light of day.

Electronic Arts Building Microtransactions Into All Future Games

EA is planning to have microtransactions in all of its future games, according to the company's chief financial officer.

Speaking at the Morgan Stanley Technology, Media, and Telecom Conference (via Develop), Blake Jorgensen claimed that the decision was made as a result of users "embracing" the controversial model.

We are building into all of our games the ability to pay for things along the way; to get to a higher level, and consumers are enjoying and embracing that way of business.

"We are building into all of our games the ability to pay for things

along the way; to get to a higher level," he explained.

"And consumers are enjoying and embracing that way of business."

Aside from the reaction this may elicit from gamers, there's the added issue of infrastructure that EA has had to consider. Jorgensen went on to explain that the company is now planning to bring all the processes surrounding payments and card-handling in-house to try and increase security.

"If you're doing microtransactions and you're processing credit cards for every one of those microtransactions you'll get eaten alive.

"And so Rajat's team has built an amazing backend to manage that and manage that much more profitably. We've outsourced a lot of that stuff historically; we're bringing that all in-house now."

Given the recent decisions regarding Dead Space 3's weapon crafting system, it's hardly surprising to discover the company is rolling this out into all its products. IGN reached out to EA, but the company declined to comment.

Goodbye, And Thank You From The GameSpy Team

GameSpy, as we know it, began in 1999. Today, 14 years later, it has reached the end of the road. We had a good run, and we want to sincerely thank all of you for reading and joining in discussions with us. It's been fantastic.

Just to be clear, we're not being shut down because PC gaming isn't a big, important, and growing thing - because it is. That's not even debatable. It's not even because the GameSpy staff did a bad job of talking about it. Hell, from where I'm sitting we did an awesome job, particularly in covering the technical quality of PC versions of cross-platform games in our Port Authority features, reality-checking the hype of about-to-be-released big games with our Questions & Concerns series, delving into the nuances of MMORPGs, strategy, MOBAs, and simulations in our columns, regularly checking up on free-to-play games in Free Agent, calling out Microsoft's neglect of PC gamers, mocking Ubisoft's claims of a day-and-date PC release of Assassin's Creed 3, breaking the news on SimCity's lack of save/reload, and of course our amazingly bizarre The War Z interview.

Why is this closure happening, then? It's a business thing, and like most business things it's not easy to explain or understand unless you spend all day crunching numbers and paying bills. Which I don't. So here's the simple version that even I can comprehend: Ziff Davis wants to run an efficient, focused company, and managing several different sites that all cover videogames isn't exactly the model of efficiency. Even though GameSpy had its own unique voice that was separate and distinct from those of our sister sites, and there has always been value in that, it's hard to argue with that logic. Even if it does totally suck.

The silver lining is that the value of all of the voices and opinions of our staff and writers won't just go away. We'll still be out there talking and writing about the great things happening in the world of PC gaming, both at IGN and other places around the internet, because it's what we

love to do. It's why we wanted to work at GameSpy in the first place. We hope you'll keep reading and watching and talking about PC games with us.

- Dan Stapleton, Editor in Chief

It's True: 1UP Has Reached Its End

The corporate version:

Today, Ziff-Davis announced that as part of a restructuring of its new property IGN Entertainment, three of IGN's smaller secondary sites - namely, 1UP.com, Gamespy.com, and UGO.com - would be "winding down." As is often the case with such reorganizations, some of 1UP's staff was laid off while others will be moving over to work as contributors at IGN.com. No timeline was given for 1UP's closure or if its servers would continue to run indefinitely.

The human version:

As of today, 1UP will be entering the sunset into which all former websites eventually must ride. This comes as huge disappointment for me - not because I'm editor-in-chief of the site, but because I've been with it since the beginning. That's nearly 10 years of my life invested in this website through all its ups and downs... and ups... and dooooowwwwwns.

It's been a fantastic (almost) 10 years. Even in its most frustrating and even dispiriting moments (there were some pretty dark times before IGN bought us in 2011), 1UP has always been fueled by the sincere enthusiasm of everyone writing for the site. Dozens upon dozens of people have moved through the various doors of our assorted offices, and each of them brought passion and talent to their work. I'm proud to have been a part of something so much larger than myself, and to help guide it as gracefully as possible to its slow halt since taking over the role left behind by my predecessors, Sam Kennedy and James Mielke.

Read through the site's archives and you'll find some truly amazing content. In-depth interviews with legendary developers, insanely detailed explorations of the niche and obscure, brilliant coverage of the top news of the day. You'll find revolutionary video programs and trendsetting podcasts. Incisive reviews and comprehensive blogs. God, there's so much here we need to archive in case someone does pull the plug on the servers.

But most of all, 1UP has always been fueled by passionate readers. No, you guys are more than readers - you're participants. You've called in for podcasts, shaken our hands at trade shows and conventions, flagged us down on the street, berated us in comments, and chimed in to express your own take on the topics of the day. 1UP has played a huge role over the years in changing the perception and nature of the gaming press from broadcast to conversation. And the outpouring of memories and affection today on forums, on Twitter, and in our blogs has only served to reinforce the impact 1UP has had on countless people. You guys are awesome.

                         =~=~=~=

     Activisionaries: How Four Programmers Changed The Game Industry

In the late 70s and early 80s, Atari was a giant in the entertainment
world. It helped kickstart the video game industry with a combination of
high-profile games and inventive hardware that invaded local bars as well
as the living room. Atari became a cultural icon and one of America s
rising industrial stars. But it didn t get there alone. As the first
third-party developer, Activision was one of Atari s biggest supporters,
producing some of the most successful and best-loved games for the ›Atari
2600. Many credit Activision with bolstering Atari hardware sales and
helping sustain the console maker s branding. Atari didn t see it that
way. To Atari, Activision was the worst kind of enemy: an enemy that had
come from within.

The Memo that Sparked a Fire

In early 1979, Atari s marketing department issued a memo to its
programing staff that listed all the games Atari had sold the previous
year. The list detailed the percentage of sales each game had contributed
to the company s overall profits. The purpose of the memo was to show the
design team what kinds of games were selling and to inspire them to create
more titles of a similar breed. Unfortunately, a few of Atari s designers
were less ›than ›inspired.

David Crane, Larry Kaplan, Alan Miller, and Bob Whitehead were four of
Atari s superstar programmers. Collectively, the group had been
responsible for producing many of Atari s most critical hits. Titles like
Canyon Bomber and Surround don t sound like much today, but over 30 years
ago they were hot properties. The four programmers also respected each
other s work, and had formed a clique within the company.

 I remember looking at that memo with those other guys, recalls Crane,
 and we realized that we had been responsible for 60 percent of Atari s
sales in the previous year   the four of us. There were 35 people in the
department, but the four of us were responsible for 60 percent of the
sales. Then we found another announcement that [Atari] had done $100
million in cartridge sales the previous year, so that 60 percent
translated into ›$60 ›million.

These four men may have produced $60 million in profit, but they were only
making about $22,000 a year. To them, the numbers seemed astronomically
disproportionate. Part of the problem was that when the video game
industry was founded, it had molded itself after the toy industry, where a
designer was paid a fixed salary and everything that designer produced was
wholly owned by the company. Crane, Kaplan, Miller, and Whitehead thought
the video game industry should function more like the book, music, or film
industries, where the creative talent behind a project got a larger share
of the profits based on its success.

The four walked into the office of Atari CEO Ray Kassar and laid out their
argument for programmer royalties. Atari was making a lot of money, but
those without a corner office weren t getting to share the wealth. Kassar

who had been installed as Atari s CEO by parent company Warner Communications   felt obligated to keep production costs as low as possible. Warner was a massive c>orporation and everyone helped contribute to the >company s >success.

 He told us, You re no more important to those projects than the person on the assembly line who put them together. Without them, your games wouldn t have sold anything,   Crane remembers. He was trying to create this corporate line that it was all of us working together that make games happen. But these were creative works, these were authorships, and he didn t >get >it.

 Kassar called us towel designers, Kaplan told InfoWorld magazine back in 1983, He said, I ve dealt with your kind before. You re a dime a dozen. You re not unique. Anybody can do >a >cartridge.

The four programmers left Kassar s office dejected. Warner was willing to give its recording artists royalties for the music they made, but their most productive programmers couldn t even get a bonus after making the company millions. Crane, Kaplan, Miller, and Whitehead were good at making games   that in-house memo proved people wanted to play what they programmed. The four decided that they were done working for Atari. But they weren t done making games for >the >Atari.

A New Kind of Company

In the 70s, when a company wanted to get into the video game business, it created a video game console and then started making games that would play on that console. Atari made game cartridges for the Atari 2600, Magnavox made games for its Odyssey system, and Mattel made games for its Intellivision. Making games for other consoles didn t make practical business sense at the time. If you wanted to make video games, you had to make a console first.

And then four dissatisfied programmers from Atari formed Activision.

 Before we started the company, we checked with lawyers to make sure that it was legal to do what we were talking about, Crane says. We actually budgeted for a lawsuit when we went to a venture capitalist and got backing. Sure enough, they tried to sue the pants off us.

Getting funding was a challenge in and of itself. At the time, venture capital firms didn t invest in software companies. Software didn t seem like a real product because there was nothing tangible to hold onto. The four programmers secured backing for their company only on the basis that they would be producing physical cartridges, which would be marketed as games. Even then, the private equity firm Sutter Hill Ventures invested less than $1 million into the company. Within three years, Activision would be worth more than $300 million.

From the beginning, Activision looked like a different kind of video game company. Crane, Kaplan, Miller, and Whitehead teamed up with a businessman named Jim Levy, and the five founded their company on the idea that a game was a piece of art created by an author. As they envisioned it, Activision would give every programmer credit on the games they made, and would even promote authors by devoting a full page to them in the instruction manual. The founders decided to package their games in bright, colorful boxes with their Activision label clearly displayed across the top so the company s games would clearly stand out on store shelves. Most importantly, the four programmers knew the Atari 2600 inside and out, so

their games used every ounce of the system s graphical capabilities.
Black borders were even employed to keep color bleeding down. Many would
later say that Activision s games looked better than many of Atari s own
titles.

Battling a Giant

By the fall of 1979, the four programmers had set up inside Crane s garage
and started working on their initial launch lineup: Dragster, Fishing
Derby, Checkers, and Boxing. The games wouldn t release until the
following summer, but to help build sales momentum for its new products,
and in order to establish its brand name, Activision took its games to
the summer Consumer Electronic Show ›in ›Chicago.

 Our first CES was quite a splash, Crane says. We were in the third
sub-basement at McCormick Place. Fortunately, we were in the corner and
we had our banner at an angle, so we had good visibility even though we
were the last booth in the last place anyone went. Even so, people saw
our booth and immediately started to ›get ›excited.

The young developer started generating so much press that Atari felt it
had to go on the offensive. On the second day of the show, Atari bought a
full page ad in the CES trade show daily aimed directly ›at ›Activision.

 It said, Atari believes that anyone who would steal trade secrets from
another company and try to profit on them are evil, terrible people,
Crane recalls. They didn t mention Activision by name, but it was pretty
clear they were talking about us. It was funny, because they made that
statement, but we all agreed with it because we weren t stealing anything.
They tried to paint us as being ›really ›bad.

Atari continued its attack, trying to bully the fledgling publisher out of
the retail market by telling retailers that they wouldn t be able to carry
Atari products if they distributed for Activision. Atari then accused
Activision of stealing various proprietary information, including a
programming trick known as the venetian ›blinds ›technique.

The venetian blinds technique had been invented by Bob Whitehead while he
was working on Video Chess for Atari. The technique allowed sprites to
change positions every scan line, meaning a programmer could get eight or
more sprites to line up onscreen. Previously, programmers had only been
able to get the Atari 2600 to produce six sprites on a single line, so
this was a nifty trick. The problem for Atari was Activision hadn t used
the venetian blinds technique in any of its games.

Atari continued to threaten to sue Activision for stealing company
secrets, so David Crane worked up a demo of a digital window overlooking a
sunset. A player could use a joystick to raise or lower a set of
venetian-style blinds attached to the window. When Atari s lawyers came
over to question the Activision crew about the venetian blinds programming
technique, Crane showed them the demo of the digital venetian blinds,
asking, Is this what you re talking about? Everyone thought it was
hilarious. Everyone except Atari s lawyers; Atari filed a ›lawsuit
alleging that Activision's members had violated a ›non-disclosure
›agreement.

 They tried all these monopolistic practices, and it was stupid because
we helped make their console the de facto standard for a decade because
we were supporting it and the next group supported it, Crane says. They
were selling more consoles because of our support, but they couldn t see

it that way. We were the best thing that could have happened to Atari, but they didn t think so at >the >time.

Activision continued to churn out a string of hits that included Kaboom!, Chopper Command, Skiing, and Pitfall! Then in 1982, Atari decided that it was losing the lawsuit and opted to settle out of court. Activision could continue to develop third-party video games for Atari s systems in return for royalties   an arrangement that functions much like modern first-party/third-party licensing agreements. The Atari 2600 was officially an open platform. Activision had swung the doors wide open for a slew of long-forgotten third party companies like Imagic, Tigervision, and Froggo Games to flood >the >market.

The Activision that exists today is a vastly different company than the one formed in David Crane s garage back in 1979. The company has weathered a series of financial losses, a name change, and a multi-million dollar patent infringement lawsuit over the years. The company s founders had all left by the mid- 80s and by the time that current CEO Bobby Kotick acquired the company, Activision was such a financial disaster that it was forced to file for Chapter 11 bankruptcy. Despite its dire straits, Activision was >worth >saving.

 What Bobby Kotick realized was that the Activision brand name was worth $50 million when he bought the company for less than $1 million, Crane says. It was estimated at that point that it would cost $50 million in marketing to make another company be as recognizable as Activision already was, so he had that going for him and he knew it.

Much of Activision s success today is built on that brand name, but its legacy is larger than a single company. Crane, Kaplan, Miller, and Whitehead envisioned an industry where game makers were credited as artistic visionaries who shared in the profits of a game s financial success. They envisioned an industry where games were not just seen as toys, but as entertainment products comparable to movies, music, and books. It was a vision of today s industry, a reality they helped shape.

Activision Timeline

    1979 (May) Atari programmers David Crane, Larry Kaplan, Alan Miller, and Bob Whitehead meet with Atari CEO Ray Kassar to demand that the company reward its developers >more >fairly
    1979 (Oct) Crane, Kaplan, Miller, and Whitehead file papers to found their own company, Activision, the first independent developer and distributor of video >game >software
    1981 (Jul) Activision releases Kaboom!, which has players using the paddle controller to capture explosives dropped by a mad bomber at the top of the screen. The game goes on to become one of the company's >early >million-sellers
    1982 (Apr) Activision releases Pitfall! The game becomes one of Activision s most iconic titles, and is often credited as the first platformer. It goes on to sell over four million copies   a dizzying feat for the Atari 2600. Later in the year, co-founder Larry Kaplan leaves for Amiga.
    1983 (Mar) The company ends its fiscal year by reaching more than $157 million in sales and by June completes its initial >public >offering
    1984 Bob Whitehead and Alan Miller leave Activision to >form >Accolade
    1986 The last remaining founder at Activision, David Crane, leaves the company to co-found Absolute Entertainment with >Garry >Kitchen
    1987 Activision purchases Infocom, the leading adventure game developer and publisher >of >Zork

1988 Activision changes its corporate name to Mediagenic and broadens
its focus to include ›business ›software
     1989 Activision, under Mediagenic, publishes the first interactive
entertainment product on CD-ROM, an adventure game for kids called ›The
›Manhole
     1990 BHK Corporation, headed by Bobby Kotick, purchases a controlling
interest ›in ›Mediagenic
     1992 (Dec) Mediagenic emerges from chapter 11 bankruptcy and changes
its name back to Activision
     2007 (Dec) Activision and Vivendi announce that they have signed a
merger agreement, effectively making them the world s largest video game
publisher. The company renames itself ›Activision ›Blizzard

                              =~=~=~=

                    A-ONE's Headline News
              The Latest in Computer Technology News
                   Compiled by: Dana P. Jacobson

          White House, Lawmakers Resume Cybersecurity Bill Talks

U.S. House Intelligence Committee Chairman Mike Rogers said on Friday
negotiations with the White House on a new cybersecurity bill have
resumed, and the two sides are not "that far apart" after making progress
this week.

The Michigan Republican told Reuters that both sides are "very close" on
agreeing about the roles that the Department of Homeland Security and
other government agencies would play to better defend against cyber
attacks.

They are also negotiating ways to minimize the transfer and use of
personal information from companies to the government, Rogers said. No
written drafts have been exchanged, the talks are informal and no deal is
imminent, a committee staffer said.

In a joint interview with the senior Democrat on his committee, Dutch
Ruppersberger, Rogers said the talks have been aided by increasing
concerns about the costs of cyber attacks.

"What helped is that The New York Times, Washington Post and Wall Street
Journal were all hacked and they talked about it publicly," Rogers said.
"It is starting to raise awareness. I can feel movement."

Though thousands of important companies have been losing data to hackers
in China and elsewhere for a decade, the number of companies publicly
admitting such breaches has been growing. Apple, Microsoft, Twitter, and
Facebook confirmed attacks in a recent campaign.

Rogers said both sides of the talks and an expanding part of the public
understand that the likelihood of a devastating destructive attack is
growing as the list of cyber powers lengthens to include actors like
Iran.

He said he had "a high degree of confidence" that Iran was behind the August 2012 attack on Saudi Aramco that crippled some 30,000 PCs.

He also blamed Iran for a campaign against banks in recent months with what are known as denial-of-service attacks, which have disrupted access to some websites, and he said more intrusive or destructive hacking could follow.

"That's a probing action," said Rogers, who is privvy to classified intelligence reports. "We know it's not the best they have to offer.

"You have this non-rational actor that has the capability to cause chaos to people's networks and could be economically destructive."

The joint bill by Rogers and Ruppersberger emphasizes sharing threat information among companies and the government. It passed the Republican-dominated House last year, but failed in the Democrat-controlled Senate after administration objections.

The White House wants a more comprehensive bill that also sets minimum security standards for vitally important companies. But Ruppersberger said last month's executive order on that issue eased some pressure to include such provisions.

A second gulf between the parties has been over the personal information on customers and users that would be turned over to the government.

The current House bill would give broad protection from lawsuits to companies that surrender user data believed to be related to "threats" to their networks to DHS, which could then share it with intelligence agencies that could use it for other national security matters.

But Rogers said the personal information was not essential. "Candidly, you don't need a lot of personal information to fight the threat," he said, adding that details of new malicious software was essential.

Ruppersberger, of Maryland, said companies complained that they had no way to "minimize" personal information attached to "millions of conversations" and that they were working through that issue in the White House talks.

Their comments follow an interview with White House cybersecurity policy adviser Michael Daniel on Monday at the same RSA conference, the largest annual gathering of security professionals.

Daniel told Reuters then that the administration would identify its goals for a new law within two months.

Only after a law passes to shore up defense, the House members said, can the country focus on building support among allies to confront economic espionage from China and others.

China Says U.S. Routinely Hacks Defense Ministry Websites

Two major Chinese military websites, including that of the Defense Ministry, were subject to about 144,000 hacking attacks a month last year, almost two-thirds of which came from the United States, the ministry

said on Thursday.

This month a U.S. computer security company said that a secretive Chinese military unit was likely behind a series of hacking attacks mostly targeting the United States, setting off a war of words between Washington and Beijing.

China denied the allegations and said it was the victim.

It has now provided some details for the first time of the alleged attacks from the United States.

"The Defense Ministry and China Military Online websites have faced a serious threat from hacking attacks since they were established, and the number of hacks has risen steadily in recent years," said ministry spokesman Geng Yansheng.

"According to the IP addresses, the Defense Ministry and China Military Online websites were, in 2012, hacked on average from overseas 144,000 times a month, of which attacks from the U.S. accounted for 62.9 percent," he said.

The comments were made at a monthly news conference, which foreign reporters are not allowed to attend, and posted on the ministry's website.

Geng said he had noted reports that the United States planned to expand its cyber-warfare capability but that they were unhelpful to increasing international cooperation towards fighting hacking.

"We hope that the U.S. side can explain and clarify this."

The U.S. security company, Mandiant, identified the People's Liberation Army's Shanghai-based Unit 61398 as the most likely driving force behind the hacking. Mandiant said it believed the unit had carried out "sustained" attacks on a wide range of industries.

The hacking dispute adds to diplomatic tension between China and the United States, already strained by Chinese suspicion about Washington's "pivot" back to Asia and arguments over issues from trade to human rights.

185 Thousand Spyware Images Sent to Rental Computers

Spyware installed on computers leased from furniture renter Aaron's Inc. secretly sent 185,000 emails containing sensitive information including pictures of nude children and people having sex back to the company's corporate computers, according to court documents filed Wednesday in a class-action lawsuit.

According to the filings, some of the spyware emails contained pictures secretly taken by the rental computers' webcams or other sensitive information including Social Security numbers, social media and email passwords, and customer keystrokes, the Federal Trade Commission determined last year.

The attorneys also claimed Atlanta-based Aaron's hasn't properly notified at least 800 customers allegedly targeted by spyware made by DesignerWare,

a company located in North East, Pa.

"Because Aaron's has been so uncooperative in agreeing to give proper notice and assistance to its customers, we've had to ask the court to intervene and order them to do it, so that people can protect their most private kinds of rights and property," said Maury Herman, a New Orleans attorney who was one of several to file the documents.

Aaron's officials have previously said the company never installed the spyware on computers rented out of company-operated stores and blamed individual franchisees for installing it. But the new filings claim Aaron's nonetheless received the secretly recorded data.

Aaron's said in a statement that it disagrees with the claims in the lawsuit and will defend the case vigorously. The company reiterated its assertion that some of its 700 franchise stores used the spyware, not the 1300-plus company-owned stores.

Attorneys for DesignerWare didn't immediately respond to a request for comment Wednesday.

The new allegations grew out of a Federal Trade Commission settlement last year and are contained in documents filed in U.S. District Court in Erie. That's where a Casper, Wyo., couple, Brian and Crystal Byrd, have sued DesignerWare, Aaron's, the local franchise from which they rented a computer in 2010, and 45 other unidentified franchises they believed were using the spyware.

The filings seek court permission to file a new complaint adding 54 franchisees based on the 185,000 emails since traced to Aaron's computer servers.

"Aaron's, like the proverbial ostrich, has buried its head in the sand, hoping this litigation would just go away without having to do anything to protect its customers," the Byrds' attorneys wrote.

The couple's May 2011 lawsuit claimed the manager of the Casper store showed Brian Byrd a webcam picture of himself operating a rental computer after the manager activated the spyware in the process of trying to repossess the computer, which the manager mistakenly believed the Byrds hadn't paid off under their rent-to-own agreement.

Attorneys for DesignerWare have since said in court documents its PC Rental Agent software is benign and simply helps rental companies track computer use and shut down the devices if customers don't pay.

But the FTC found, in a settlement publicized in September, the software could do much more when "Detective Mode" was activated: Capturing screenshots, taking webcam images, logging keystrokes and forwarding that information to Aaron's by email.

The FTC settlement bars DesignerWare, the Aaron's franchise that operated the Wyoming store, and six other businesses that operated rental stores from using any location-tracking software without customer consent and from deceptively collecting information.

On Wednesday, attorneys for the Byrds also filed a new lawsuit in Fulton County, Ga. where Atlanta is located on behalf of a customer who claims an Oregon Aaron's franchise tracked her physical location by having Detective Mode trace her WiFi use of the computer.

That lawsuit, and the new documents filed in the Byrd's federal lawsuit, contends Aaron's corporate officials condoned the widespread use of the spyware on franchise rental computers.

Apple s Deleting iCloud Emails That Contain The Phrase Barely Legal Teens

Apple has a well documented history of banning everything that has anything to do with pornography, even if it s only remotely related. It s nice that Apple wants to keep the App Store clean, but their obsession with eliminating porn from computing has a lot of collateral damage.

In its latest push to get porn off your computer, Apple now deletes all iCloud emails that contain the phrase barely legal teens. It doesn t send the messages to spam, or flag them, it just straight up deletes them, and there s nothing you can do about it.

It sounds like Apple s just trying to help you avoid child pornography, but the iCloud censorship was actually discovered by an Academy Award-winning screenwriter named Steven G., who has nothing to do with child porn.

Steven G. wrote to InfoWorld that his software was trying to send a script to a director by emailing it from an iCloud account. The director never got the script, so Steven sent it multiple times as he tried to figure out why the email was getting blocked.

Eventually, Steven started cutting the script down into pieces to see which sections of the attached script were getting flagged and blocked.

AND THEN I SAW IT a line in the script, describing a character viewing an advertisement for a pornographic site on his computer screen. Upon modifying this line, the entire document was delivered with no problem.

Maybe it s just a coincidence, but Steven took his testing even farther. He created a PDF containing the line: All my children are barely legal teens why would I want to let them drive by themselves? And yep, Apple s servers sent the attachment straight to hell. Then he just typed that phrase in a regular email and it was blocked too.

After more research, Steven found that under the iCloud terms of service, Apple reserves the right to remove any content at any time that it feels is objectionable, without telling you that they re going to delete it. Apparently, barely legal teens falls into that objectionable content category, along with other phrases we re probably not aware of.

We ran our own quick tests that seemed to back up Stevens claims. Apple was asked to confirm whether it s actively scanning files in iCloud and deleting them if they have keyword phrases like barely legal, but they haven t responded.

Net Providers Begin Warning of Illegal Downloads

Internet users who are illegally sharing music, movies or television shows are going to start to receive warning notices from the nation's five major Internet service providers.

The Copyright Alert System, organized by the recording and film industry, is being activated this week to target consumers who may be engaging in piracy using peer-to-peer software.

Under the new system, complaints will prompt an Internet service provider — such as Verizon or AT&T — to notify a customer whose Internet address has been detected sharing files illegally. A person will be given up to six opportunities to stop before the Internet provider will take more drastic steps, such as temporarily slowing their connection. Proponents say the focus is on educating consumers. They acknowledge it's unlikely to deter chronic violators.

Why Corporate Twitter Accounts Get Hacked

Earlier this week, Internet users were treated to another reminder that some of the world's biggest brands don't have the firmest of grasps on their Twitter accounts.

On Monday (Feb. 18), the Burger King Twitter account was hijacked, resulting in a stream of foul-mouthed, funny tweets about how the company had been bought by rival McDonald's.

On Tuesday, it was Jeep's turn, with a string of tweets promoting mostly obscure rappers. (MTV's own Twitter hijack later Tuesday turned out to be a marketing stunt.)

Why are so many corporate Twitter accounts being hacked and hijacked?

Easy-to-guess passwords are initially to blame, but experts said poor passwords indicate a bigger problem: Many big companies simply just don't take social media seriously.

"When senior management doesn't understand social media, they sometimes feel very comfortable handing over social-media management to interns or recent graduates," Philadelphia-based social-media strategist Alexandra Golaszewska told TechNewsDaily.

While the Jeep and Burger King Twitter hijacks were hilarious to many, such incidents can seriously harm a brand's relationship with its customers by showing that brand managers don't value the direct connections social media provides.

"If the decision makers don't use [social media] themselves, they might not understand the extent of its reach," Golaszewska said. "They don't always realize that even a deleted post can live forever in screen shots."

Dismissive attitudes toward social media can lead to lax social-media security as well. High turnover and unclear social-media policies may result in many former interns and employees who still have keys to a company's social-media platforms.

No one has ever died from a hacked Twitter account or a disgruntled

intern's rant on the corporate Facebook profile, but that doesn't mean these incidents don't have real-life consequences.

In the past couple of years, household names such as KitchenAid, Chrysler, Microsoft, Marc Jacobs and StubHub have had their Twitter accounts abused by employees who thought they were tweeting on their own personal accounts, or who used the corporate account to send offensive or brand-damaging messages to a larger audience.

It's not just companies that are at risk. Several celebrities, including Ashton Kutcher, Miley Cyrus and Britney Spears have had their accounts taken over by hackers who suddenly find themselves with an unearned audience of millions.

So how can an individual or company protect a Twitter account?

"In addition to creating a strong password, be sure to change your password often and always change it after someone leaves the company," said Rebecca Debono, social-media strategist at San Diego digital-marketing agency Digitaria. "You never know where former employees place old documents online or how easy their accounts are to hack."

"I always say to my clients, if you can remember your password, it is not cryptic enough," San Diego social-media expert and consultant Mari Smith told TechNewsDaily. "People need to do their homework and find a reliable system that stores passwords and gets them out of the habit of committing passwords to memory."

Smith recommends social-media scheduling tools such as HootSuite, which enables multiple people to tweet or post updates on a single account but doesn't allow users to make profile changes.

"Following these simple guidelines significantly reduces your likelihood of falling victim to a public hacking experience," Debono said.

Smith pointed out that if Twitter offered two-step authentication and strongly encouraged users especially high-profile celebrities and brands to enable it, account hijacks such as these would happen with less frequency.

(Twitter has said it is looking into adding two-step authentication, which would require users to log in with a password and a separate factor, such as a code text-messaged to a mobile phone.)

But OneID founder Steve Kirsch, whose service provides one username and password for multiple online accounts, disagrees.

Kirsch told tech news service ZDNet this week that even if Twitter offered two-step authentication, he doesn't believe it would be widely adopted.

"From a practical point of view, it would be like offering a feature that no one used," Kirsch said.

It's true that even the strongest passwords and authentication methods wouldn't have prevented a recent attack that resulted in the theft of 250,000 Twitter passwords.

In that case, hackers exploited a flaw in Oracle's Java browser plug-in to break into Twitter's employee network. (Twitter subsequently changed the

passwords of all affected users.)

There's no panacea that will solve the complex security problems of navigating the corporate world on social media.

But companies may be doing themselves a disservice if they treat social media as a second-rate medium for communicating with their customers. As with any other customer-facing aspect of a business, image and control is everything.

In Death, Facebook Photos Could Fade Away Forever

A grieving Oregon mother who battled Facebook for full access to her deceased son's account has been pushing for years for something that would prevent others from losing photos, messages and other memories   as she did.

"Everybody's going to face this kind of a situation at some point in their lives," says Karen Williams, whose 22-year-old son died in a 2005 motorcycle accident.

The Oregon Legislature responded and took up the cause recently with a proposal that would have made it easier for loved ones to access the "digital assets" of the deceased, only to be turned back by pressure from the tech industry, which argued that both a 1986 federal law and voluntary terms of service agreements prohibit companies from sharing a person's information   even if such a request were included in a last will and testament.

Lobbyists agree the Stored Communications Act is woefully out of date but say that until it's changed, laws passed at the state level could be unconstitutional.

"Everybody wants to do the right thing, but the hard legal reality is the federal communications act," said Jim Hawley, a vice president at TechNet, an industry group that represents companies such as Google and Microsoft.

Oregon lawmakers moved ahead anyway with a proposal that would have given "digital assets"   everything from photos and messages stored online to intellectual property and banking information   the same treatment as material property for estate purposes.

"I think it's time for us to really look at what we can do now," said Democratic Sen. Floyd Prozanski after hearing Williams testify about her loss last month.

Two weeks later, however, language in the bill that would have covered social media accounts, from Facebook to Flikr, was stripped as tech lobbyists said the federal law and company privacy policies trumped anything that the bill would have included.

"I recognize the emotional toll these types of decisions can have on a family who's lost a loved one," Prozanski said Thursday. "But some of these issues may have to be addressed when we have more information than we currently have."

Still, the problem persists and discussions on the issue are gaining

momentum. As unlikely as such a case might be, even if a person willingly gives over login and password information to someone whom they authorize to access a given digital account, it would violate most terms of service agreements and both people could be charged with cybercrimes and face civil action from Internet companies under current law.

Currently, five states have digital assets laws, which vary widely. This group includes Oklahoma, which passed a law two years ago allowing estate lawyers to access digital assets, even social media accounts. That measure did not face the opposition that has emerged in Oregon.

"There is some question if laws like the one we passed in Oklahoma, would stand up to a challenge by Facebook and Gmail saying their terms of service agreements supersede laws like this one and the one being discussed in Oregon," said Ryan Kiesel, a former Oklahoma legislator who wrote the law.

"That's a question that remains to be answered," he added.

Several other states, including Nebraska   guided in part by the story of Williams' 22-year-old son, Loren   are also considering proposals. And the Uniform Law Commission, a non-profit, non-partisan group that writes model legislation for states to help standardize laws around the nation, is examining the issue.

"This law is a real need as we have moved into a digital world," said Lane Shetterly, an Oregon attorney and a representative on the commission's drafting committee. The group is responsible for standardizing a range of legislation, including commercial transaction regulations and child custody laws.

Proponents say the need is clear. Without clarity or direction, the digital information left behind by a deceased person can spark emotional legal battles, pitting big business against devastated families. And as more and more memories are being stored online, new tools are necessary to make sure loved ones can easily access personal details that could be lost forever.

"If this were a box of letters under his bed, no one would have thought twice," Williams said.

Months after the death of her first-born son, who was away at college in Arizona, Williams found comfort in his Facebook page. There, she was able to click through photos and letters that helped ease the pain of her loss   for two hours.

She learned of the page from his friends and wanted access to his memories to keep them from being deleted, which was Facebook's policy at the time. Unaware of Internet privacy regulations, she reached out to Facebook for help. As she waited for a response, one of his friends provided a tip that helped her discover his password. "It was like a gift," she said.

Shortly after, however, the site's administrators changed the password, citing company policy in denying her. Williams sued and won, but she never received the full access she sought. Eventually, the account was taken down. In the end, she gained little more than a symbolic victory and a role as champion of a cause that didn't exist before the digital age.

Kiesel, the former Oklahoma lawmaker, says the various attempts at legislation have sparked a long overdue conversation about estate

planning for digital assets.

"I think that, because of the wide prevalence of online accounts and digital property, the federal government will ultimately need to pass some legislation that provides greater uniformity," he said.

Congress, however, has no current plans to take up the matter. U.S. Sen. Mark Pryor, an Arkansas Democrat who heads the Senate Commerce Subcommittee on Communications and Technology, is not planning to introduce any digital assets proposals and has not heard any come up, his press secretary said. Also, a bill aimed at modernizing the Stored Communications Act failed in the House Judiciary Committee last year.

"This is not going to happen overnight," said Greg Nojeim, of The Center for Democracy and Technology, a Washington-based non-profit, public policy group. He said changes to the Stored Communications Act were being discussed by industry groups, "but none that would help these families."

Under current law, Internet companies that provide storage for digital assets are prohibited from disclosing account information, even to families, without a court order, which can be costly and difficult to obtain.

Even then, there are no guarantees. Facebook, for example, citing its terms of service agreement won't provide access, even if a judge orders them to do so. Facebook will not comment on pending legislation or specific cases other than to defer to their service agreement, which states, in part, "We may access, preserve and share your information in response to a legal request (like a search warrant, court order or subpoena) if we have a good faith belief that the law requires us to do so."

Along these lines, TechNet, one of several groups in opposition to the Oregon measure, provided written testimony arguing that legislation requiring online companies to provide access could subject them to federal criminal penalties.

"We just want to make sure that whatever comes out doesn't put a company in a position where they have to choose between state and federal law," said Hawley.

The pending Oregon legislation now covers only digital assets of commercial or financial value such as online banking information.

"It's absolutely devastating," Williams said.

Since she began her quiet crusade after her 2007 court victory yielded limited, temporary access to her son's account, the social media landscape has changed considerably, but there is still no industry standard. Where Facebook once deleted the accounts of deceased users, for example, pages can now be memorialized for public view.

Many predict the problem will grow as long as there are no estate laws in place to determine what happens to virtual property left behind by the deceased.

Without a clear law, estate managers can be charged with cybercrimes for attempting to access clients' digital accounts, said Victoria Blachly, a Portland attorney who helped draft the initial Oregon proposal.

Estate planning attorney James Lamm writes about the issue on his blog "Digital Passing." He advises clients to include explicit instructions in their wills stating exactly how digital assets should be handled   even if there is no guarantee those wishes will be carried out.

"It's good to come up with a thoughtful plan for what happens to all of your property," he said. "Your physical properties, and your digital properties."

 Google Spent $18 Million Lobbying D.C. in 2012, Apple Spent $2 Million

The last time we looked at Silicon Valley's lobbying efforts, Google was the big spender and Apple the piker.

That hasn't changed much in the past nine months. In fact, Google increased its political spending in 2012 - a Presidential election year - by nearly 90%, while Apple reduced its by 13%.

(The biggest percentage increase, by the way, was Facebook's. It upped its D.C. spending nearly 200%, from $1.35 million to just under $4 million.)

Where did Apple spend its $2 million? According to the company's LD-2 disclosure form, the money was spread out pretty thinly over a wide range of issues, among them:

    Taxation (including the repatriation of profits earned overseas)
    Education (including the use of digital textbooks in schools)
    Telecommunications (including open Internet and children protection issues)
    Environment (including electronic waste, Energy Star and EPEAT standards)
    Trade (including free trade and border issues)
    Consumer Issues (including privacy protection and the Do Not Track Me Online Act)
    Investments and the SEC (including implementation of the Dodd-Frank Act)
    Transportation (including the use of technology in cars and airplanes)
    Computer Industry (including cybercrime)
    Appropriations (including government precurement rules)
    Media (including electronic publishing)
    Medical (including the regulation of mobile medical devices)

Meanwhile, I recommend once again This American Life's Take the Money and Run for Office. It's a fascinating inside look at big-time lobbying that will change the way you look at Washington politicians.

        Google s New $1,299 Laptop Can t Run Office, Photoshop

Thanks to Google, there's now a way to save a couple hundred dollars on buying a 13-inch Retina MacBook Pro. All you have to do is make it a tiny bit smaller, move most of its storage space online to Google Drive, and take away the ability to run practically any apps. Instead, you're going to be going to websites like Google's for pretty much everything.

That, at least, is one way of looking at Google's new first-party laptop, the Chromebook Pixel. Unlike previous Asus and Samsung Chromebooks, this one is 100 percent Google, and gives us a pretty good idea of how Google thinks laptops should be. It's a very different idea from Apple or Microsoft's, however.

Like Apple's MacBook series, the Chromebook Pixel is made from an aluminum unibody. It's a bit more squared-off than theirs, but still looks more high-end than most PC laptops.

The screen has a 3:2 aspect ratio, which means that it isn't widescreen. On the other hand, its 239 ppi (pixels per inch) display is a bit sharper than the 13-inch Retina MacBook Pro's, partly because it's a bit smaller. It's also a touchscreen, although you can't fold or twist it back and use it like a tablet the way you can some Windows 8 laptops. Instead, you have to reach up and touch the screen.

How about the Chromebook Pixel's internals? It has a dual-core, 1.8 GHz Intel Core i5 processor with integrated graphics, 4 GB of RAM, and a 32 GB solid state drive which will mostly be used for caching offline websites. The LTE Chromebook costs $150 more, and has a 64 GB solid state drive plus a couple years' worth of free LTE from Verizon (only 100 MB per month though).

It does come with one terabyte of storage on Google Drive, the company's Dropbox clone which has Google Docs integration. Upload speeds are very slow for most people with residential Internet connections, however, so it'd take awhile to backup your existing files there. It's also a limited-time offer which lasts for three years, so if you want to extend it you'll need to either pay $49.99 a month afterwards or buy another Chromebook.

Chromebooks like the Chromebook Pixel use the Chrome Web Store for app purchases. Most of the "apps" there are websites, but some are actually full games (like Bastion) and apps which run in the browser, using technologies like Javascript and Chrome's Native Client.

Will you find familiar PC and Mac apps like Microsoft Office and Photoshop? Not really, no. Both have online versions, that you can go to in Chrome even if they aren't in the web store. But those lack most of the features of their offline counterparts.

For typical use, a Chromebook Pixel can do most of the things people normally do with "computers," although it helps if you spend most of your time in a browser already. Most professionals, though, or even serious PC/Mac gamers, would be hard-pressed to make it their primary computer, because the games and apps simply aren't there.

Windows 8 Fails To Impress Holiday Shoppers

Following the seemingly tepid launch of Windows 8, critics were told to wait until after the holiday shopping season was over to properly assess Microsoft s (MSFT) newest operating system. The latest monthly numbers from analytics firm Net Applications are in and Windows 8 usage remains low. After two months into the new year, the operating system only accounts for 2.67% of web traffic, a small increase from 2.36% in

January. Windows 8 continues to lag behind Windows Vista (5.17%),
Windows XP (38.99%) and Windows 7 (44.55%). Last month also marked the end
of Microsoft s deep discount on Windows 8. The operating system now costs
a whopping $119.99, making it even more difficult for the company to
entice consumers to upgrade.

IE10 for Windows 7 Globally Available for Consumers and Businesses

Internet Explorer 10 is available worldwide in 95 languages for download
today. We will begin auto updating Windows 7 customers to IE10 in the
weeks ahead, starting today with customers running the IE10 Release
Preview. With this final release, IE10 brings the same leading standards
support, with improved performance, security, privacy, reliability that
consumers enjoy on Windows 8, to Windows 7 customers.

With IE10 we continue delivering the best performance for real world Web
sites on your Windows device. As with Windows 8, IE10 on Windows 7
improves performance across the board with faster page loading, faster
interactivity, and faster JavaScript performance, while reducing CPU usage
and improving battery life on mobile PCs. In measurements in our
performance lab, IE loads real world pages up to 20% faster in top sites
for news, social, search, ecommerce, and more.

You can experience IE10 s leading performance first hand with demos on the
IE Test Drive site with examples of hardware accelerated rendering,
interactivity, touch, and real world site patterns. Minesweeper is a new
test drive demo that is both a full featured HTML5 game and also lets you
measure your browser s performan

Minesweeper is built on a breadth of Web platform capabilities including
HTML5, CSS3, WOFF, touch, animations, transitions, audio, video, canvas,
transforms, and power efficiency patterns. The game uses standards-based
mark-up for interoperability across browsers, and makes the most of fully
hardware accelerated browsers like IE10 on both Windows 7 and Windows 8,
with consistent performance across a wide range of devices including
tablets like the Surface RT. Minesweeper s performance mode measures how
long it takes the browser to solve the minesweeper board, so you can test
your browser performance with different minesweeper boards with different
complexity.

IE10 also improves hardware accelerated performance of SVG and HTML4
constructs. You can see improvements yourself with the Chalkboard test
drive where performance improves over IE9 by 15%. Similarly, improved
drawing performance enables faster rendering patterns you can experience
yourself with the Speed Reading test drive where performance improves by
30% over IE9 on comparable hardware.

IE10 continues to lead on JavaScript performance with many improvements to
the Chakra JavaScript engine including profile-based, type-specialized JIT
machine code, faster floating point operations, faster object and property
access, and more. All of these improvements come to IE10 on Windows 7 and
are consistent across the underlying operating system and hardware. As a
result, with IE10 on Windows 7, performance on the WebKit SunSpider
JavaScript benchmark improves by 25% over IE9 and leads the industry and
other browsers by 17%.

In addition to raw performance improvements of real world sites, IE10

includes improvements to make common browsing activities you do every day faster. IE10 s integrated spell checking and auto-correct for common spelling mistakes, makes typing text for blog posts, social updates, and tweets faster and less error prone. Similarly, we tuned the tabs bar so closing many tabs is faster and more efficient, without having to moving your mouse as each tab closes.

For developers, IE10 brings increased support for modern Web standards powered by hardware acceleration to enable a new class of compelling applications and fast and fluid Web browsing. IE10 adds support for over 30 new modern Web standards beyond IE9, for a 60% increase. These new supported standards in IE10 include many of the latest HTML5, CSS3, DOM, Web Performance, and Web Application specifications across important aspects of Web development including:

Create rich visual effects with CSS Text Shadow, CSS 3D Transforms, CSS3 Transitions and Animations, CSS3 Gradient, and SVG Filter Effects
More sophisticated and responsive page layouts with CSS3 for publication quality page layouts and responsive application UI (CSS3 grid, flexbox, multi-column, positioned floats, regions, and hyphenation), HTML5 Forms, input controls, and validation
Enhanced Web programming model for better offline applications through local storage with IndexedDB and the HTML5 Application Cache; Web Sockets, HTML5 History, Async scripts, HTML5 File APIs, HTML5 Drag-drop, HTML5 Sandboxing, Web workers, ES5 Strict mode support.
Beautiful and interactive Web applications with support for several new technologies like CSS3 Positioned Floats, HTML5 Drag-drop, File Reader API, Media Query Listeners, Pointer Events, and HTML5 Forms.
Improved Web application security with the same markup and support for HTML5 Sandbox for iframe isolation.

In keeping with our commitment on prioritizing the privacy of our customers, the Do Not Track (DNT) signal is turned on in IE10 for Windows 7. In addition to Tracking Protection, IE continues to lead in providing increased choice and control over your privacy online. Customers can choose to turn-off the DNT signal in the options settings in Internet Explorer.

Our commitment to keeping Windows customers in control of their privacy and data sharing continues, especially in the current environment of so much user data being collected online without explicit consent or user awareness.

The opportunities continue for HTML5 to make both Web sites and applications better. Those opportunities are exciting for everyone on the Web. Like IE10 on Windows 8, this release brings high performance HTML5 development to Windows 7.

For developers building on HTML5, now is time to get ready for IE 10. Developers can use the recently launched modern.IE to test and verify your sites, using a wizard that scans a Web page URL for common interoperability problems and suggests some ideas for how to address those issues to improve the user experience across modern and older browsers.

On behalf of the individuals and companies who have worked with us to deliver this product, and the many people at Microsoft who have built it, thank you for your feedback and for using IE10.

Internet Advertisers Kill Text-based CAPTCHA

If you've submitted a comment, signed up for a newsletter, or uploaded a photo to the Internet at any point in the past five years, there's a good chance you're familiar with the CAPTCHA system. CAPTCHAs are the annoying little verification windows that pop up, asking you to decipher a nearly unrecognizable series of letters or words, and Web users have hated them for years. But if these silly security systems make you want to bust your keyboard in half, you'll be happy to hear that we may very well be seeing the last days of the obnoxious, text-based CAPTCHA system, and the next verification system you see online may make you happy to view advertisements for the first time ever.

Rather than taking just a mere glance to figure out, recent studies show that a typical CAPTCHA takes, on average, 14 seconds to solve, with some taking much, much longer. Multiply that by the millions and millions of verifications per day, and Web users as a whole are wasting years and years of their lives just trying to prove they're not actually computers. This has led many companies to abandon the age-old system in favor of something not only more secure, but also easier to use for your average Webgoer: Ad-based verification, which can actually cut the time it takes to complete the task in half.

Now when performing a Web task, such as purchasing event tickets from Ticketmaster, for example, you may no longer be met with a swirling mix of letters and numbers, but instead by an advertisement or common brand logo. Rather than demanding that you decipher a completely pointless combination of fuzzy words, you could simply be asked to recite a well-known company slogan. The security pop-up might even ask you to view an ad image and then type the company's name.

The new system is turning out to be a big time saver for just about everyone, and Web users are typically able to confirm their humanity much faster than with the standard verification tool. New York-based Solve Media one of the leaders of the ad-based verification revolution claims the ads it uses for user confirmation take about seven seconds to complete, cutting wasted time in half.

But ad-based verification isn't the only revolutionary idea looking to usurp the standard CAPTCHA's throne. Both puzzle and math-based variations on the tool have also started to gain traction. Puzzle versions of the tool ask you to perform a simple task, like draw a circle around a specific object in an image, while the mathematical option requests that you solve some simple arithmetic. Both of these variants allow you to confirm your humanity without deciphering a garbled string of text, but they lack the revenue-generating capability of the ad-based method. And because of this added monetary bonus of the commercial model, both the puzzle and math verification tools have less of a chance of becoming commonplace.

CAPTCHA which stands for "Completely Automated Public Turing test to tell Computers and Humans Apart" first gained prominence in the early 2000s as a way to keep Web forms from being spammed by computer bots. It's impossible to tell how much time Web users as a whole have wasted as a result of the increasingly difficult text strings, but with much simpler alternatives finally beginning to catch on, it appears that the fuzzy text nonsense is finally meeting its end. Advertisements in general are usually seen as a hindrance to daily life, but in this case, ads will actually make your life easier. What a novel concept!

UK Kids Turn to Google Instead of Grandparents for Advice

British grandparents are in danger of being overlooked for advice by their grandchildren, who are more accustomed to searching for answers on the internet, a survey showed on Thursday.

Almost nine out of every 10 UK grandparents claimed their grandchildren failed to ask them for advice for simple tasks, instead turning to online channels such as Google, YouTube and Wikipedia for information.

Answers on how to boil an egg, iron a shirt and even details on their own family history are now easily found by younger generations glued to their smartphones, tablet computers or laptops, according to research commissioned by cleaning products firm Dr Beckmann.

"Grandparents believe they are being sidelined by Google, YouTube, Wikipedia and the huge resource of advice available on the internet," spokeswoman Susan Fermor said in a statement.

"They are aware that their grandchildren, already with their noses buried in a laptop, tablet computer or smartphone, find it much easier to search the internet for instant advice."

The survey of 1,500 grandparents also found that children chose to research what life was like for their elderly relatives in their youth rather than asking the grandparents themselves, with just 33 percent of grandparents having been asked: 'What was it like when you were young?'.

Almost two-thirds of grandparents felt their traditional roles were becoming less and less important in modern family life, with 96 percent claiming that they asked far more questions of their own grandparents when they were young.

=~=~=~=

not necessarily reflect those of the staff, or of the publishers. All
material herein is believed to be accurate at the time of publishing.